Chukhleb Marina Vladimirovna
Student
Ural Federal University named after the first
President of Russia B.N. Yeltsin
Russia, Ekaterinburg
Academic supervisor: Tkacheva Marina Viktorovna

ETHICAL HACKING

Abstract. *The article focuses on ethical hacking. This article considers the social norms that the ethical hacker follows. It also describes the most commonly used testing method - penetration testing.*

Keywords: *ethical hacking, hacker, penetration testing, security, system vulnerabilities.*

Чухлеб Марина Владимировна
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Ткачева Марина Викторовна

ЭТИЧНЫЙ ХАКИНГ

Аннотация. *Статья акцентирует внимание на этичном хакинге. В статье рассматриваются общественные нормы, которыми руководствуется этичный хакер. Также описывается наиболее используемый метод тестирования - тестирование на проникновение.*

Ключевые слова: *Этичный хакинг, хакер, тестирование на проникновение, безопасность, уязвимости системы.*

Introduction

Ethical hacking is a new necessity in today's world. Companies began to possess a large volume of confidential information, the loss of which can lead to a huge damage and loss of trust among users. News about system breaches from large companies becomes the subject of debate. It makes these companies pay more attention to security policy and new opportunities for fixing problems in architecture. Therefore, the need for the ability to use security tools and vulnerability analysis has led to the creation of courses and schools for ethical hacking. The word «hacker» should not scare companies away. On the contrary, bringing ethical hackers to the company will improve the company's security and reduce the risk of cyberattacks that can lead to information leakage.

1. What is a hacker?

According to the Oxford Dictionary, a hacker is a person who uses computers to get access to data in somebody else's computer or phone system without permission. Indeed, the first association with hackers is that they are cybercriminals who steal users' personal information, data for their own benefit. However, it is worth introducing another definition of the word hacker. A hacker is just a person who uses computer programming or technical skills to overcome a challenge or problem [1]. A number of security professionals use the techniques and mindsets of hackers to learn, test, and fix technologies.

Among specialists, the division of hackers into white, grey, and black hats has become entrenched.

White hats, or in other words ethical hackers, help companies to find and fix holes in security. Such hackers act in the public interest. Many hackers work on penetration testing. After testing, they announce security weaknesses to the company.

For the general public black hats are cybercriminals who gain unauthorised access to sites and networks with malevolence intention. It can be like stealing

confidential information, spreading viruses, or DDoS (A Distributed Denial of Service) attacks. The main goal of such hackers is profit. Black hats are real criminals because by their actions they violate the laws on illegal access to computer information, the creation of malware.

Hackers in grey hats are usually not motivated by money and have no criminal intentions. They sit somewhere on the line between a bad hacker and a good hacker.[2]

2. Ethical hackers

Ethical hackers are hackers that are hired by companies that want to get an assessment of their security system. Ethical hackers follow a formal set of rules. An ethical hacker acts like a cybercriminal, but the goal is not to harm the company. The hacker looks for vulnerabilities that can be in-used by criminals. Essentially, a hacker's assessment of the security of a system should answer the questions: «What information can hackers get?», «What can be done with this information?» and «What information will go unnoticed» [3].

Ethical hackers adhere to a strict code of conduct that protects their relationship with their clients and the interests of their clients. It describes the rules that must be followed. These rules help to establish a relationship of trust between the client and the hacker.

For white hats, customer trust is paramount. It is important for the company that an ethical hacker does not abuse his access to the system. After all, when a company provides some information, an ethical hacker can discover commercial secrets and confidential data. In this case, the hacker must understand that he must work in accordance with the law [4].

An ethical hacker must apprehend that he can receive a fine for illegal hacking into the system. Ethical hacking activities related to a network-penetration check or security audit should not be started until a signed official document allowing the white hat to take the hacking activities is received from the organisation.

For hackers, there is a special programme called Big Bounty. This programme offers an award for detecting security issues in a company's service and applications.

This programme is implemented in such large companies as Google, Facebook, Apple, Microsoft, etc.

3. Penetration testing

Penetration testing, or pentesting, is the practice of analysis of the system for vulnerabilities. [5]. According to the degree of automation, testing is divided into manual and automated.

According to the study by Positive Technologies, in 93% of companies, pentesters managed to get access to the local network, and a sixth of the firms checked had traces of previous attacks [6]. In this way, a penetration test identifies security shortcomings and vulnerabilities that hackers can find.

Organisations use this type of testing to validate the security policy that has been implemented in the company. White hats give feedback after testing and reporting weaknesses found in a system, companies can reallocate resources to their IT security section. Also, the error report will be useful for programmers and IT-specialists of the company to prevent analogous errors afterward.

Ethical hackers use automated tools to recognise vulnerabilities. Many pentesting tools are free and open-source software. The popular free tools are Nmap, Wireshark, John the Ripper.

White hats and cybercriminals use basically the same tools. One of the reasons why white hats use the similar instruments is that they are freely available on the network. Also, the usage of the same tools for pentesting explains better the way of how they can be brought into play against an organisation.

Hackers can have varying amounts of information about the system they scan. Thus, a hacker can either have full access to the code or have no information at all about the contents of the architecture diagram. Therefore, the following testing approaches are distinguished: white box, grey box, and black box.

Black box testing assumes that the test engineer is a hacker who does not know the target testing system. The maximum data that a tester can own are the IP-address

and the company's website. A penetration tester should be familiar with automatic scanning tools and has manual penetration testing skills. This testing approach is an expensive option because in this case, the hacker must view himself as an attacker who spends time learning about various elements before attacking the system.

A grey box is a mixture of white and black boxes. In this case, the tester has little knowledge of the system.

A white box pentest is a pentester who possesses the maximum amount of information, architecture documentation, etc. This is a laborious testing since a huge amount of code and data must be examined to discover weaknesses. When testing a white box, an ethical hacker must own code debuggers.

The most thorough of the three methods reviewed is the white box method. Since it includes an analysis of the source code, this allows you to recognise the largest number of problems. In comparison, the black box permits you to look at problems more broadly, however, the lack of information about the system leads to the omission of security vulnerabilities [7].

Conclusion

Being a white hat or an ethical hacker is a safe way to work and make money.

The main area for a hacker is penetration testing. The special bug bounty programme is a good opportunity for pentesters to earn money. To participate in these programmes successfully, it is important to adhere to ethical standards, as well as to the rules set by the company.

A successful career as an ethical hacker requires advanced programming skills to analyse systems in search of vulnerabilities and skills in using specialised testing tools.

REFERENCES

1. What is a hacker. – Text: electronic. – URL: https://www.webroot.com/us/en/resources/glossary/what-is-a-

hacker#:~:text=A%20hacker%20is%20just%20a,many%20different%20types%20of%20hackers (Reference date 25.11.2020)

2. What is the Difference Between Black, White and Grey Hat Hackers? – Text: electronic. – URL: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html (Reference date 25.11.2020)

3. Scott Nicholson. How ethical hacking can protect organizations from a greater threat. – Computer Fraud & Security. 2019. P 15-19.

4. David-Olivier Jaquet-Chiffelle and Michele Loi. Ethical and unethical haching. – The Ethics of Cybersecurity. 2020. P 179-204

5. Pen test (penetration testing) – Text: electronic. – URL: https://searchsecurity.techtarget.com/definition/penetration-testing (Reference date 27.11.2020)

6. External pentests results – 2020. – Text: electronic. – URL: https://www.ptsecurity.com/ww-en/analytics/external-pentests-results-2020/ (Reference date 27.11.2020)

7. What are Black Box, Grey Box, and White Box Penetration Testing? – Text: electronic. – URL: https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/ (Reference date 30.11.2020)